K-Shield Jr. C 반

OO 웹사이트 모의해킹 수행계획서

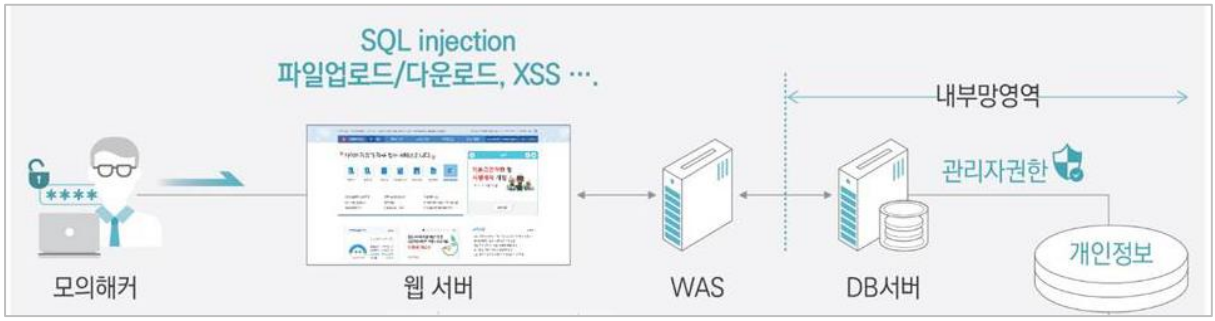
2020-10-26

목차

1 배경 및 목적

본 취약점 진단은 OO 웹사이트에 대해 "주요정보통신기반시설 기술적 취약점 상세 가이드" 진단 항목을 기준으로 존재하는 취약점을 발견하고 취약점을 증명함으로써 해킹 위협으로부터 안전성 여부를 판단함과 동시에 보안 대응책을 강구함을 목적으로 한다.

2 수행 범위



팀명	진단 사이트
1팀	OO 웹 사이트1
2팀	OO 웹 사이트2

[표 2-1] 모의해킹 수행 범위

3 수행 전략

- 작업의 효율성을 위해 취약점 진단 시 2인 1조로 구성하여 한 조당 하나의 취약점을 점검하도록 한다.
- 미리 취약점 별 공격 스크립트를 작성하여 목록화하고, 프로젝트를 수행하는 시간에는 목록화된 코드를 대입하여 수행 시간을 최소화한다.
- 매일 프로젝트 수행 전, 전 날 파악된 취약점을 기반으로 팀원 한 명당 1개의 시나리오를 계획한다.

4 수행 일정

<2020. 10. 26(월) ~ 2020. 11. 4(수)>

수행일정	26(월)	27(화)	28(수)	29(목)	30(금)	2(월)	3(화)	4(수)
수행계획서 작성								
정보 수집								
취약점 진단								
모의 침투								
보안대책 수립								
결과 보고서 작성								
프로젝트 발표								

[표 4-1] 모의해킹 수행 일정

5 수행 인원

팀	성명	비고
모의해킹 1팀	박기택	PL, 팀장
	김일한	
	강경훈	
	임승원	
	함도윤	
모의해킹 2팀	정형수	팀장
	김재원	
	이호웅	
	김상훈	

[표 5-1] 모의해킹 수행 인원

6 수행 내용

6 - 1 수행기준

점검항목	항목 중요도	항목코드
버퍼 오버플로우	상	BO
포맷스트링	상	FS
LDAP 인젝션	상	LI
운영체제 명령 실행	상	OC
SQL 인젝션	상	SI
SSI 인젝션	상	SS
XPath 인젝션	상	XI
디렉터리 인덱싱	상	DI
정보 노출	상	IL
악성 콘텐츠	상	CS
크로스사이트 스크립팅	상	XS
약한 문자열 강도	상	BF
불충분한 인증	상	IA
취약한 패스워드 복구	상	PR
CSRF	상	CF
세션 예측	상	SE
불충분한 인가	상	IN
불충분한 세션 만료	상	SC
세션 고정	상	SF
자동화 공격	상	AU
프로세스 검증 누락	상	PV
파일 업로드	상	FU
파일 다운로드	상	FD
관리자 페이지 노출	상	AE
경로 추적	상	PT
위치 공개	상	PL:
데이터 평문 전송	상	SN
쿠키 변조	상	CC

6 - 2 수행 내용 상세

6 - 2 - 1 정보수집

- OSINT를 활용한 웹 정보를 수집한다.

  * SHODAN : https://www.shodan.io/

  * Censys : https://censys.io/

- 정보 수집 도구를 활용하여 웹 정보를 수집한다.

수집 도구	사용 목적
whatweb	서버의 구성요소 및 사용된 기술 식별
Nmap	네트워크 스캐닝

6 - 2 - 2 취약점 진단

- 주요정보통신기반시설 취약점 가이드를 기반으로 웹 취약점 진단을 수행한다.
- 취약점 진단을 통해 확인된 취약점을 목록화한다.

6 - 2 - 3 모의 침투

- 파악된 취약점 목록을 활용하여 시나리오를 수립한다.
- 수립한 시나리오를 기반으로 모의 침투를 진행한다.
- 침투 결과에 따른 웹 서비스 안전성 확보 방향을 제시한다.

7 기대효과

- 홈페이지 모의해킹을 통한 데이터 유출 가능성 사전탐지 및 예방
- 주요정보통신기반시설 취약점 가이드를 포함하는 웹 해킹 취약점 해소를 통한 안전성 확보
- 개인정보 유출 등의 해킹 사고 발생시 법적 책임 완화
- 홈페이지 취약점 발견을 통해 위험도 측정을 통한 대응방안 제시
- 고객에게 안정적 서비스를 제공하여 기업 이미지 향상